



FortiClient (Linux) - Release Notes

Version 6.0.3

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<https://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



October 29, 2018

FortiClient (Linux) 6.0.3 Release Notes

04-603-513774-20181029

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's New in FortiClient (Linux) 6.0.3	6
Basic USB device control	6
Installation Information	7
Installing FortiClient (Linux)	7
Installing FortiClient (Linux) from repo.fortinet.com	7
Installing FortiClient (Linux) using a downloaded installation file	8
Installation folder and running processes	8
Uninstalling FortiClient (Linux)	8
Product Integration and Support	10
Resolved Issues	11
Malware Protection	11
GUI	11
Other	11
Known Issues	12
Endpoint Control	12
Malware Protection	12
Vulnerability Scan	12
GUI	12
Other	13

Change Log

Date	Change Description
2018-10-18	Initial release.
2018-10-29	Updated Installation Information on page 7 .

Introduction

FortiClient (Linux) 6.0.3 is an endpoint product for well-known Linux distributions that provides FortiTelemetry, Antivirus, and Vulnerability Scan features. FortiClient (Linux) can also download and use FortiSandbox signatures.

This document provides a summary of support information and installation instructions for FortiClient (Linux) 6.0.3 build 0073.

- [What's New in FortiClient \(Linux\) 6.0.3 on page 6](#)
- [Installation Information on page 7](#)
- [Product Integration and Support on page 10](#)
- [Resolved Issues on page 11](#)
- [Known Issues on page 12](#)

Review all sections prior to installing FortiClient.

What's New in FortiClient (Linux) 6.0.3

This section identifies the new features and enhancements in FortiClient (Linux) 6.0.3. For more information, see the *FortiClient Administration Guide*.

Basic USB device control

You can use the USB device control feature to restrict access to USB ports on endpoints.

Installation Information

Installing FortiClient (Linux)

You can install FortiClient (Linux) on the following operating systems:

- Red Hat
- CentOS
- Ubuntu

For supported versions, see [Product Integration and Support](#) on page 10.



To install a FortiClient (Linux) 6.0.3 RPM package, you must first uninstall any earlier version of FortiClient (Linux) installed. It is not supported to upgrade to FortiClient (Linux) 6.0.3 using the RPM package.

Installing FortiClient (Linux) from repo.fortinet.com

You can install FortiClient (Linux) from the repository at repo.fortinet.com.

Installing on Red Hat or CentOS

1. Add the repository by using the following command:

```
sudo yum-config-manager --add-repo http://repo.fortinet.com/repo/centos/7/os/x86_64/fortinet.repo
```
2. Install FortiClient by using the following command:

```
sudo yum install forticlient
```

Installing on Ubuntu

1. Install the gpg key by using the following command:

```
wget -O - http://repo.fortinet.com/repo/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```
2. Add the following line in `/etc/apt/sources.list`:

```
deb [arch=amd64] http://repo.fortinet.com/repo/ubuntu/ xenial multiverse
```
3. Update package lists by using the following command:

```
sudo apt-get update
```
4. Install FortiClient by using the following command:

```
sudo apt install forticlient
```

Installing FortiClient (Linux) using a downloaded installation file

Installing on Red Hat or CentOS

1. Obtain a FortiClient Linux installation rpm file.
2. In a terminal window, run the following command:

```
$ sudo yum install <FortiClient installation rpm file> -y
```

<FortiClient installation rpm file> is the full path to the downloaded rpm file.

Installing on Ubuntu

1. Obtain a FortiClient Linux installation deb file.
2. Install FortiClient using the following command:

```
$ sudo apt-get install <FortiClient installation deb file>
```

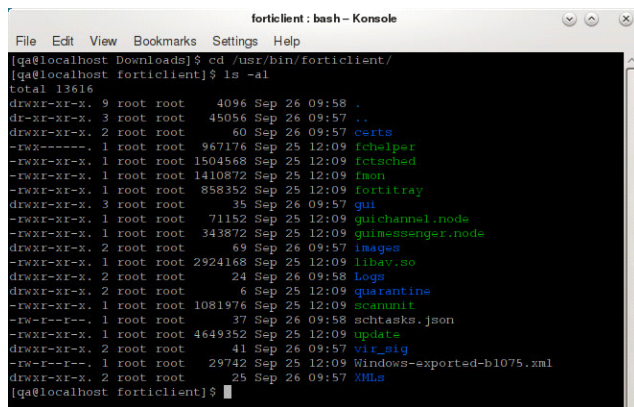
<FortiClient installation deb file> is the full path to the downloaded deb file.

Installation folder and running processes

FortiClient installation folder is /usr/bin/forticlient.

```
config.xml is in /etc/forticlient
```

In case there are issues, or to report a bug, FortiClient logs are available in `/var/log/forticlient`.



Some running processes `/usr/bin/forticlient` include:

- fctsched
- fortitray
- FortiClient
- epctrl

Uninstalling FortiClient (Linux)

Use the following procedure to uninstall FortiClient (Linux) from Red Hat or CentOS operating systems.

To uninstall FortiClient:

1. In a terminal window, run the following command:

```
$ sudo yum remove forticlient
```

Use the following procedure to uninstall FortiClient (Linux) from Ubuntu operating systems.

To uninstall FortiClient:

1. In a terminal window, run the following command:

```
$ sudo apt-get remove forticlient
```

Product Integration and Support

The following table lists version 6.0.3 product integration and support information.

Operating Systems	<ul style="list-style-type: none">• Ubuntu 16.04 and later• Red Hat 7.4 and later• CentOS 7.4 and later All supported with KDE or GNOME
FortiClient EMS	<ul style="list-style-type: none">• 6.0.0 and later
FortiOS	<ul style="list-style-type: none">• 6.0.0 and later• 5.6.0 and later
FortiSandbox	<ul style="list-style-type: none">• 3.0.0 and later• 2.5.0 and later• 2.4.0 and later• 2.3.3 and later

Resolved Issues

The following issues have been fixed in version 6.0.3. For inquiries about a particular bug, contact [Customer Service & Support](#).

Malware Protection

Bug ID	Description
508488	FortiClient (Linux) AV log does not provide any summary about threats found, AV engine, and signature.
509225	FortiTray color does not change to yellow when in standalone mode.
510292	FortiClient (Linux) sends the wrong serial and version numbers to Sandbox in the OFTP messages.
510336	FortiClient (Linux) does not send the EMS serial number in OFTP message to Sandbox.
516253	FortiClient (Linux) stops generating AV logs when log level is changed to Information.

GUI

Bug ID	Description
490469	The Linux host hangs after AV quarantines eicar for a few times.

Other

Bug ID	Description
510365	FortiClient (Linux) Endpoint Control logs keep showing debug logs when FortiClient (Linux) log level is set to Information.
516394	FortiClient (Linux) freezes on the patching progress screen and also causes the host machine to hang up.

Known Issues

The following issues have been identified in FortiClient (Linux) 6.0.3. For inquiries about a particular bug or to report a bug, contact [Customer Service & Support](#).

Endpoint Control

Bug ID	Description
518060	FortiClient (Linux) cannot disconnect from EMS when dually registered to a second EMS via a gateway list.

Malware Protection

Bug ID	Description
503202	FortiClient does not report AV events to EMS.

Vulnerability Scan

Bug ID	Description
518777	FortiClient (Linux) is unable to patch vulnerabilities on CentOS.

GUI

Bug ID	Description
506389	FortiClient shows "Vulnerabilities scanned 0" during patching.
516224	GUI keeps showing scheduled scan on AV page when it is disabled.

Other

Bug ID	Description
458729	Administrator cannot define multiple FortiAnalyzer units for remote logging.
481618	CentOS 7.4: FortiClient (Linux) does not report an event in the log file when it blocks USB.
495409	FortiClient does not start vulnerability scan when it gets a signature update.
505552	Cannot export logs from FortiClient (Linux).
510517	FortiClient (Linux) does not check compliance for running applications and processes.



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.